(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
13. Januar 2005 (13.01.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/003933 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, 17/30

(21) Internationales Aktenzeichen: PCT/DE2004/001252

(22) Internationales Anmeldedatum:
17. Juni 2004 (17.06.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 29 779.0 1. Juli 2003 (01.07.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: KÖPPEN, Siegried [DE/DE]; Chausseestr. 60, 15711 Königs-Wusterhausen (DE). LÖWE, Stefan [DE/DE]; Kaiserin-Auguste-Allee 95, 10589 Berlin (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente)R8-10, Am Kavalleriesand 3, 64295 Darmstadt (DE).

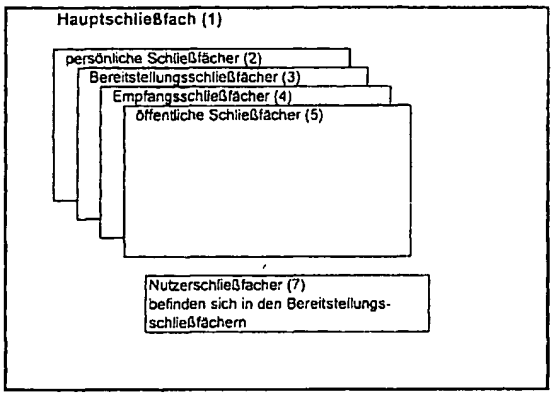
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

*[Fortsetzung auf der nächsten Seite]*

(54) Title: METHOD FOR USE IN A NETWORK BASED SAFETY DATA STORAGE SYSTEM

(54) Bezeichnung: VERFAHREN FÜR EIN NETZBASIERTES DATENSPEICHERSYSTEM MIT HOHER SICHERHEIT




(57) Abstract: The invention relates to a method for use in a data storage system which applies high safety requirements for the storage of data on a server in a telecommunications network and for the retrieval of the files by the local computers linked with the server via the network. The applicant is provided with a user certificate and public and secret keys, preferably on a chip card. Once the server is dialed up via the internet, a client program is forwarded to the user which controls authentication of the user and the transmission of additional safety-relevant features of proof such as biometrical systems, geographical positioning, time-dependent data, network and computer data etc. to the server. The storage system on the server is provided with a locker-type characteristic by establishing folders comprising a specific file for the safety requirements related thereto. The lockers are distinguished by their specific function and are only displayed to the user when the safety requirements are met. This locker system thus also has virtual character.

*[Fortsetzung auf der nächsten Seite]*

WO 2005/003933 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

**(57) Zusammenfassung:** Die Erfindung betrifft ein Verfahren für ein Datenspeichersystem, bei dem für die Speicherung der Daten auf einem Server in einem Telekommunikationsnetz und den Abruf der Dateien durch die über das Netz mit dem Server verbundenen lokalen Rechner hohe Sicherheitsanforderungen vorgegeben werden. Nutzerzertifikat sowie öffentlicher und geheimer Schlüssel werden dem Antragsteller vorzugsweise auf einer Chipkarte bereitgestellt. Nach Anwahl des Servers über das Internet wird dem Nutzer ein Clientprogramm zugesandt, das die Authentifizierung des Nutzers sowie die Übertragung weiterer sicherheitsrelevanter Nachweise wie biometrische Systeme, geografische Positionsbestimmung, Zeitabhängigkeiten, Netz- und Rechnerdaten u.a. zum Server steuert. Das Speichersystem auf dem Server erhält Schließfachcharakter, indem jeder Ordner mit einer speziellen Datei für die auf ihn bezogenen Sicherheitsanforderungen eingerichtet wird. Die Schließfächer werden nach Funktionen unterschieden und kommen für die Nutzer nur zur Anzeige, wenn die Sicherheitsbedingungen erfüllt sind. Damit hat Schließfachsystem einen virtuellen Charakter.

10/563337
IAP20 Rec'd PCT/PTO 03 JAN 2006



**Verfahren für ein netzbasiertes Datenspeichersystem mit hoher Sicherheit**

**Beschreibung**

Die Erfindung betrifft das Gebiet der Sicherheit für den Zugriff und die Datenspeicherung auf Servern, die in Netzwerken mit freiem Zugang arbeiten.

Angaben zum Stand der Technik

Für die Sicherheit und Bereitstellung von Dateien über z.B. das Internet gibt es eine Reihe von Anwendungen, deren spezifische Merkmale im folgenden dargestellt werden.

Bei der Applikation Cryptoheaven (siehe http://www.crytoheaven.com) handelt es sich um eine Java Applikation (Applet/Java Plugin). Die Anzeige erfolgt wie beim MS-Explorer, links geteilt in Verzeichnisbaum (incl. lokaler Rechner) und Kontaktliste. Einstellungen sind über die rechte Maustaste/Popup möglich. Es wird ein proprietäres Protokoll über den Port 82 verwendet. Eingesetz wird Datenkompression. Dateien werden signiert und verschlüsselt. Ein Upload der Dateien ist auch mit Drag and Drop (DnD) aus dem lokalen Filesystem möglich. Die Ablaufsteuerung entspricht weitgehend der von MS-Explorer. Die Verschlüsselung erfolgt lokal auf dem Clientrechner. Es können Verzeichnisse angelegt, gelöscht und umbenannt werden. Die Freigabe von Verzeichnissen erfolgt an "eingeladene Nutzer". Die Einladung über e-mail erfolgt durch Teilnehmer, die das System abboniert haben. Der Eingeladene muss zustimmen. Die Authentifizierung erfolgt mittels User-ID und Passwort. Das System gibt es für die Betriebssysteme Windows/Unix und Linux.

Eine andere typische Anwendung gibt es bei bvPREMIERE, bvPRO, bvPLUS+ und big VAULT Enterprise (siehe http://www.bigvault.com). Die Anwendungen sind speziell für Windows und ermöglichen die Einbindung (Anlegen) eines Laufwerks in den MS-Explorer, der über das WEB bedient wird. Das Übertragungsprotokoll für Dateiupload und Dateidownload ist html über eine SSl-Verbindung. Die Verschlüsselung der Dateien erfolgt auf dem Server. Die Freigabe von Verzeichnissen und Dateien erfolgt mit einem Besucherpasswort. Es gibt einen Eingangskorb für autorisierte Nutzer. Ein Login ist als Nutzer oder Besucher möglich. Das Einrichten von Passwörtern mit beschränkter

Gültigkeitsdauer erfolgt in der Art, wie es beispielsweise bei UNIX seit vielen Jahren angewendet wird.

Eine weitere Anwendung, die einen online Datei-Service für Upload/Download bietet, ist GLOBEDESK (siehe http://www.globedesk.com). Für Upload/Download über den Browser wird html oder ftp verwendet. Die Verbindung wird über SSL gesichert. Die Verschlüsselung erfolgt auf dem Server. Die Namen der Abonnenten sind in einem Verzeichnis aufgelistet. Ein Klick auf einen Namen verbindet mit den bereitgestellten Verzeichnissen. Die Identifizierung der Nutzer erfolgt über e-mail und Namen.

Die angegebenen Beispiele sind durch folgende Merkmale charakterisiert:

- Die Sicherheit beruht auf einem Modell mit Nutzernamen und Passwort. Sobald sich ein Nutzer durch seinen Namen und das dazu gehörende Passwort authentifiziert hat, steht ihm das System in immer gleicher Weise zur Verfügung.

- Die Speicherung der Daten erfolgt in einem Dateisystem bzw. derart, das für den Nutzer die Funktionalität eines Dateisystems exakt nachgebildet wird (z.B. Postfächer bei Webmail).

Die bekannten Anwendungen haben hinsichtlich Sicherheit und Speichersystem folgende Nachteile:

- Ein auf Nutzernamen und Passwort beruhendes Sicherheitsmodell kann für die Zugriffserlaubnis lediglich die Zustände erteilt oder entzogen umsetzen. Eine feinere Einstellung, zum Beispiel durch Zeitbegrenzung oder einzuhaltende Zeitabstände für den Zugriff sind nicht möglich, ebenso nicht eine Begrenzung der Anzahl gleichzeitig zugreifender Nutzer.

- Das verwendete Speichemodell ist charakterisiert als Registratur der angelegten Ordner, in die die Dateien ohne Berücksichtigung ihrer Typen abgelegt und unverändert wieder entnommen werden. Eine frei gewählte Zuordnung nach Inhalten kann vom System selbst nicht kontrolliert werden. Völlig unmöglich ist es, dass ein Ordner von sich aus aktiv wird und beispielsweise Sicherheitskopien von den gespeicherten Dateien anfertigt, die Dateien mit einem Zeitstempel versieht oder nach vorgegebenen Speicherfristen wieder löscht.

Die Erfindung stellt sich die Aufgabe, für den Zugang und die Datenspeicherung bei Servern in Telekommunikationsnetzen ein Verfahren anzubieten, das die Nachteile der bekannten Anwendungen überwindet und eine wesentlich höhere Sicherheit gewährleistet.

Das Verfahren ist dadurch charakterisiert, das für die Zugangsrechte Abhängigkeiten wie Aufenthaltsort, Zugangszeit, Endgerätemerkmale, Qualität der Verbindungswege, Authentifizierungsmethode etc. berücksichtigt werden können und für die Datenspeicherung eine Sicherheitskonfiguration nachbildet werden kann, die dem Schließfachprinzip entspricht. Die Sicherheit wird des Weiteren dadurch erhöht, dass die Ver- und Entschlüsselung der Dateien auf dem lokalen Rechner des Nutzers erfolgt und auf dem Server noch ein zweiter Verschlüsselungsalgorithmus angewendet wird, den der Nutzer nicht beeinflussen kann.

Der Datentransfer hat das Ziel, Daten in Speichern von Servern abzulegen, um sie zu gegebener Zeit wieder auf den lokalen Rechner zurückzuholen, sie auf einen entfernten Rechner bearbeiten zu lassen, oder sie Dritten – oder dem Nutzer selbst – an einem anderen Ort für einen bestimmten Zeitraum bereitzustellen. Die Bedingungen, unter denen ein Zugriff möglich ist, müssen sich präzise einstellen und verwalten lassen. Für die Ablage der Dateien ist ein Ordnungssystem erforderlich, das eine überschaubare Übersichtlichkeit für das Auffinden der Dateien bieten sollte und die Datensicherheit optimal unterstützt.

Die Forderungen nach einer präzisen Zugriffskontrolle und einem Ordnungssystem für die Ablage der Dateien mit hoher Sicherheit werden optimal erfüllt durch das erfindungsgemäße Datenspeichersystem.. Das Datenspeichesystem umfasst den in einem Telekommunikationsnetz arbeitenden Server mit seinem speziellen Programm sowie die über das Netz einbezogenen lokalen Rechner. Das Programm auf dem Server verwendet als Speichermodell ein Schließfachsystem.. Das Schließfachsystem hat virtuellen Charakter, weil in Abhängigkeit von den Zugriffsrechten dem Nutzer nur die Schließfächer und Dateien angezeigt werden, für die der Nutzer die Zugriffsberechtigung hat. Für den Nutzer gibt es kleine Information, wenn der Zugriff verweigert wird, sondern

die Schließfächer, Unterschließfächer und Dateien, für die der Nutzer keine Berechtigung hat, werden dem Nutzer nicht angezeigt.

Für den Zugang zu dem Server und die Nutzung der Programme ist eine Erlaubnis notwendig, die von dem Betreiber des Servers erteilt wird. Ein Antrag dafür ist etwa auf schriftliche Anforderung oder über das Internet erhältlich. Der Antrag muss alle Informationen enthalten, die für die Ausstellung eines Nutzerzertifikats notwendig sind. Das Zertifikat enthält unter anderem den öffentlichen Schlüssel des Nutzers. Zu diesem öffentlichen Schlüssel besitzt der Nutzer einen geheimen Schlüssel. Vorzugsweise sind geheimer Schlüssel und Zertifikat auf einer Chipkarte gespeichert, da so ein starker Schutz des geheimen Schlüssels erreicht wird. Wird diese Möglichkeit gewählt, erhält der Nutzer, um gegebenenfalls das System ohne Chipkarte nutzen zu können, ein zweites Schlüsselpaar, bei dem der geheime Schlüssel mit einem vom Nutzer gewählten Paßwort geschützt ist.

Zur Identifikation des Nutzers werden persönliche Daten zusammen mit einer Kopie des Zertifikats in eine Datenbank eingetragen. Der Server greift auf diese Informationen zu, um Nutzer authentifizieren zu können, und um ein für alle Nutzer erreichbares Nutzerverzeichnis anzubieten. Insbesondere besitzt jeder Nutzer einen eindeutigen Systemnamen, der sich von seinem natürlichen Namen unterscheiden kann.

Bei der Anmeldung richtet der Betreiber des Servers dem Nutzer einen persönlicher Bereich des DS ein, der Hauptordner (1) des Nutzers genannt wird.
Betriebssysteme und Datenbanken speichern Daten und ihre Vewaltungsinformationen auf unterschiedlichste Weise. Hier wird zur Beschreibung das bekannte Modell der Ordner (auch: Verzeichnisse) und Dateien vewendet. Eine Datei (enthält die Daten) ist stets in einem Ordner enthalten, der entweder der sogenannte Wurzelordner ist oder selbst in einem Ordner enthalten ist. Von diesem Ordner ausgehend gelangt man so über eine Kette von Oberordnern zu dem Wurzelordner. Die Namen der Ordner in dieser Kette werden zu dem sogenannten Pfad der Datei aneinandergehängt. Eine Datei wird eindeutig durch ihren Namen und ihren Pfad beschrieben.
In dem hier beschriebenen Datenspeichersystem enthält jeder Ordner eine spezielle Datei, die Sicherheitsinformationen und Verwaltungsinformationen für den Server enthält

(Tabelle 1). Unter einem Schließfach wird im Folgenden die Einheit von Ordner und der speziellen Datei verstanden.

In dem Hauptschließfach (Hauptordner) befinden sich von dem Betreiber eingerichtetete, nach Funktionen unterschiedene weitere Schließfächer, unter anderem persönliche Schließfächer (2), Bereitstellungsschließfächer (3), Empfangsschließfächer (4), öffentliche Schließfächer (5) für den Nutzer, und ein Systemschließfach (6), zu dem nur der Server Zugang hat. Die Angabe der Schließfachart erfolgt in der zugehörigen speziellen Datei.

Ein Verweis auf eine Datei enthält mindestens den Namen derjenigen Datei, auf die sie verweist.

In persönlichen Schließfächern speichert der Nutzer nur Verweise auf seine Dateien, die übertagenen Dateien selbst speichert der Server in dem Systemordner. In Bereitstellungsschließfächern speichert der Nutzer Verweise auf seine Dateien für andere Nutzer, in Empfangsschließfächern befinden sich ihm von anderern Nutzern angebotene Verweise, und in öffentlichen Schließfächern befinden sich Verweise auf Dateien, die allen Nutzern angeboten werden. In jedem Schließfach eines oben genannten Typs kann der Nutzer Unterschließfächer einrichten, in denen er Verweise speichern kann, und die wieder andere Unterschließfächer enthalten können.

Der Zugang zu dem Server erfolgt vom lokalen Rechner aus durch Anwahl der Internetadresse des Servers. Dadurch erhält der Server die Internetadresse des lokalen Rechners. In der Regel identifiziert der Netzwerkbetreiber, der den Zugang des lokalen Rechners an das Internet vermittelt, die Zugangstelle (ISDN oder ADSL Verbindung, GSM, GPRS, WLAN, UMTS) eindeutig. Damit der Server diese Information erhält, muss unter Umständen ein Vertrag zwischen Netzwerkbetreiber und Betreiber des Datensicherungssystems bestehen, und der Netzwerkbetreiber muss die technischen Möglichkeiten bereitstellen.

Der Server schickt ein spezielles Programm auf den lokalen Rechner, das sogenannte Clientprogramm. Es ist auch möglich, ein Clientprogramm auf dem lokalen Rechner zu installieren und aus ihm heraus die Anwahl durchzuführen. Das Clientprogramm verbindet sich mit einigen auf dem lokalen Rechner vorhandenen Systemen, zum Beispiel einem Chipkartenleser, einem Fingerabdruckscanner, einem

Gesichtserkennungssystem, einem GPS Modul oder einem zur Bestimmung (oder näherungsweisen Bestimmung) des geographischen Orts eingerichtetn Systems.
Mit Hilfe des Clientprogramms kann der Nutzer die ihm auf Serverseite zur Verfügung gestellten Funktionen nutzen und die zur Ausführung der Programme notwendigen Daten eingeben, sofern er sich ihm gegenüber erfolgreich authentifizieren kann. Zur Authentifizierung bietet das Clientprogramm nach Art der vorhandenen Komponenten (Kartenleser, biometrisches System) dem Nutzer verschiedene Möglichkeiten (Name/Paßwort, PIN, Chipkarte, Chipkarte mit Biometrie) an. Die ausgewählte Methode, Ergebnis der Authentifizierung, und die geographischen Daten (sofern vorhanden) werden an den Server weitergeleitet. Schlägt die Authentifizierung fehl, trennt der Server die Verbindung, und das Clientprogramm beendet sich. Bei Erfolg kann der Nutzer wählen, ob er als normaler Nutzer (Standardzustand) oder als Administrator agieren möchte. Im zweiten Fall kann das Clientprogramm eine erneute, qualitativ hochwertige Authentifizierung wie etwa mit Chipkarte und Biometrie verlangen.

Der Zeitraum von Authentifizierung bis beenden des Clientprogramms wird Sitzung genannt. Eine erfolgreiche Authentifizierung bewirkt insbesondere, dass mit der Sitzung der Systemname des Nutzers verbunden wird. Dadurch können viele parallel ablaufende Sitzungen separiert werden, und Server und Clientprogramm können die Rechte eines Nutzers zum Ausführen von Anwendungen kontrollieren. Die vom Clientprogramm übermittelten Informationen wie Art der Authentifizierung (Name/PW, Chipkarte, ...) und geographischer Ort sowie die dem Server bekannte Anfangszeit, die aktuelle Zeit und die Adresse (Internetadresse oder Netzwerkbetreiberidentifikation) des lokalen Rechners gehören ebenfalls zu den Sitzungsdaten und werden von dem Server gespeichert.

Das Clientprogramm zeigt dem Nutzer den Inhalt seines Hauptschließfachs und seines lokalen Dateisystems in der von dem Microsoft Explorer bekannten Form als Ordnerbaum an; auch die Handhabung lehnt sich an den Explorer an. Es werden jeweils nur die Schließfächer und Verweise angezeigt, für die der Nutzer in der aktuellen Sitzung die Berechtigung besitzt. Die Berechtigung stellt der Server fest, indem er die in der speziellen Datei enthaltenen Daten mit den Sitzungsdaten vergleicht.
Die Schließfächer werden durch ein eigenes graphisches Symbol dargestellt, um sie von gewöhnlichen Ordnern zu unterscheiden. Besitzt der Nutzer Administratorrechte, erhalten die Schließfachsymbole eine besondere Farbe.

Die spezielle Datei eines Schließfachs ist nie sichtbar und kann auch nicht sichtbar gemacht werden. Ist der Nutzer Administrator, so zeigt ihm das Clientprogramm auf Anforderung den (vom Nutzer) änderbaren Inhalt der speziellen Datei an und ermöglicht ihm, Einträge zu ändern.

Das Systemschließfach ist nie sichtbar. Diese Eigenschaft kann auch nicht geändert werden, da der Nutzer keinen direkten oder indirekten Zugang zu der speziellen Datei des Systemschließfachs hat.

Das Ablegen einer auf dem lokalen Rechner befindlichen Datei in dem persönlichen Schließfach des Nutzers ist ein mehrstufiger Vorgang, der von ihm mit Hilfe eines Programms durchgeführt wird, das eine Komponente in dem Clientprogramm und eine Komponente auf dem Server besitzt. Die Benutzeroberfläche des Clientprogramms ermöglicht dem Nutzer, die abzulegende Datei durch Pfad und Namen auszuwählen und den Zielpfad in seinem persönlichen Schließfach anzugeben. Der Server informiert das Clientprogramm über Anforderungen, die das Zielschließfach an abzulegende Dateien stellt. Dazu gehören maximale Größe, bestimmtes Format (doc, pdf) oder Vorliegen einer Signatur der Daten. Sind die Anforderungen erfüllt, lädt das Clientprogramm die in der Datei enthaltenen Daten und erzeugt eine Zufallszahl, den so genannten Zugangsschlüssel (8), mit dem die Daten mit einem symmetrischen Verschlüsselungsverfahren verschlüsselt werden. Anschließend wird dieser Zugangsschlüssel mit dem öffentlichen Nutzerschlüssel zu dem verschlüsselten Zugangsschlüssel (9) verschlüsselt und der Zugangsschlüssel wird vernichtet. Dadurch wird erreicht, dass nur der Nutzer, der mit Hilfe seines geheimen Schlüssels den Zugangsschlüssel zurückgewinnen kann, den verschlüsselten Inhalt der Datei wieder entschlüsseln kann.

Dateiname, Dateityp, Dateigröße, verschlüsselte Daten und verschlüsselter Zugangsschlüssel werden zusmmen mit weiteren, nach Tabelle 2 benötigten daten, an den serverseitigen Programmteil geschickt.

Dieser verschlüsselt die Daten ein zweites Mal mit einem eigenen symmetrischen Schlüssel, so dass selbst ein Diebstahl der Daten, des verschlüsselten Zugangsschlüssels und des geheimen Nutzerschlüssels keinen Zugang zu den Daten ermöglicht. Dann erzeugt er einen systemweit eindeutigen Dateiidentifikator, der als interner Name der verschlüsselten Daten verwendet wird. Unter diesem Namen werden die verschlüsselten Daten im Systemschließfach abgelegt. Im Zielordner wird dann ein Verweis mit dem

Namen der Datei als Dateinamen erzeugt, der den Dateiidentifikator, den verschlüsselten Zugangsschlüssel und Informationen über die Datei (Größe, Typ) enthält.

Will der Nutzer als Eigentümer einer Datei diese einem anderen Nutzer anbieten, richtet er als Administrator in einem Bereitstellungsschließfach ein Nutzerschließfach (7) für ihn ein. Der Server stellt ihm dafür über das Clientprogramm in der Art eines Telefonbuchs ein Nutzerverzeichnis zur Verfügung, aus dem er den gewünschten Nutzer als Adressat auswählt. Er kann auch einer Gruppe von Nutzern ein persönliches Schließfach einrichten. Der Server trägt diesen oder diese Nutzer als Miteigentümer des Schließfachs in die Eigenschaftendatei ein.
Mit Hilfe der Benutzeroberfläche des Clientprogramms teilt der Eigentümer dem Server die anzubietende Datei und ihr Ziel (ein vom Eigentümer eingerichtetes Unterschließfach) innerhalb des Nutzerschließfachs mit. Das Clientprogramm schickt diese Informationen an den Server. Der Server prüft, ob die Eigenschaften des Zielschließfachs die gewünschte Operation erlauben, und schickt dann eine Kopie des Verweises auf die Datei zusammen mit dem öffentlichen Schlüssel des Adressaten an das Clientprogramm zurück. Dieser entnimmt aus dem Verweis den verschlüsselten Zugangsschlüssel, fordert den Nutzer auf, mit seinem geheimen Schlüssel den Zugangsschlüssel wieder herzustellen und verschlüsselt ihn dann mit dem öffentlichen Schlüssel des Adressaten zu einem neuen verschlüsselten Zugangsschlüssel. Der Zugangsschlüssel wird vernichtet, der neue verschlüsselten Zugangsschlüssel in den Verweis eingetragen, und der Verweis an den Server zurückgeschickt, der ihn in dem Zielschließfach ablegt. Dann wird in einem Empfangsschließfach des Adressaten ein Schließfach mit dem Namen des Eigentümers erzeugt.
Dadurch hat nun der Adressat einen Verweis auf die Datei zusammen mit einem persönlichen Zugangsschlüssel verschlüsselten Zugangsschlüssel.

Öffnet der Nutzer ein Empfangsschließfach, sieht er Schließfächer, die mit den Namen von Anbietern bezeichnet sind. Öffnet er ein solches Schließfach X (durch Klick auf das Icon in der Anzeige seines Clientprogramms) eines Anbieters, so durchsucht der Server die Bereitstellungsschließfächer des Anbieters nach Nutzerschließfächern, die von ihm für den Nutzer eingerichtet wurden, und wählt darunter die Nutzerschließfächer aus, die unter den aktuellen Sitzungsdaten dem Nutzer den Zugang gestatten. Diese Namen sendet der Server an das Clientprogramm, das sie als Unterschließfächer von X anzeigt. Die

Nutzerschließfächer sind also nicht wirklich in X enthalten, der Nutzer kann das aber nicht feststellen.

Die angebotenen Verweise (der Nutzer sieht angebotene Dateien) werden vom Server nur dann an das Clientprogramm gemeldet, wenn kein Sitzungsdatum die in dem Verweis verzeichneten Bedingungen verletzt.

Aus der Beschreibung wird deutlich, dass ein Nutzer einen Verweis höchstens dann in seinem Clientprogramm sieht, wenn der Verweis einen mit dem öffentlichen Schlüssel des Nutzers verschlüsselten verschlüsselten Zugangsschlüssel enthält. Der Nutzer kann mit seinem geheimen Schlüssel und dem verschlüsselten Zugangsschlüssel den Zugangsschlüssel der Datei wiederherstellen und die verschlüsselten Daten entschlüsseln.

| | | | | | |
|---|---|---|---|---|---|
| Eigentümer: | | | | | |
| Erstellungsdatum: | | | | | |
| Recht „betreten“ Mitbenutzer 1: | Ort a<br>...<br>Ort z | Zeit a<br>...<br>Zeit z | Auth a<br>...<br>Auth z | | |
| Recht „betreten“ Mitbenutzer n: | „ | „ | „ | | |
| | | | | | |
| Obere Schranken: | Dateigröße einzeln | Dateigröße Summe | Anzahl Unterschließfächer | | |
| Einschränkungen: | Dateityp | | | | |

**Tabelle 1: spezielle Ordnerdatei**

| | | |
|---|---|---|
| Definition: | Vom System angelegte Datei;<br>Repräsentant einer Datei im Systemschließfach | |
| Datenfelder: | Identifikator der verwiesenen Datei;<br>Verschlüsselter Verschlüsselungsschlüssel;<br>Typ der Datei;<br>Größe der Datei;<br>Zeit der Dateierzeugung;<br>Zeit der Anlage des Verweises;<br>Zeit des letzten Zugriffs. | |
| Sicherheitsinformationen: | Eigentümer;<br>Restriktion Authentifizierung | |
| | | |

**Tabelle 2: Verweis**

**Verfahren für ein netzbasiertes Datenspeichersystem mit hoher Sicherheit**

Patentanspruch

1. Verfahren für ein netzbasiertes Datenspeichersystem mit hoher Sicherheit, bei dem die Speicherung der Daten auf einem Server in einem Telekommunikationsnetz erfolgt und die lokalen Rechner der Nutzer über das Telekommunikationsnetz mit dem Server verbunden sind, **dadurch gekennzeichnet.**
   - dass der Betreiber des Servers dem Nutzer auf Antrag ein Nutzerzertifikat für die Zugangsbedingungen ausstellt, das in Verbindung mit einem öffentlichen und einem geheimen Schlüssel dem Nutzer vorzugsweise auf einer Chipkarte bereitgestellt wird,
   - dass der über das Internet angewählte Server ein Clientprogramm zum lokalen Rechner des Nutzers sendet, das für den Nutzer die Authentifizierung mit der Chipkarte sowie die Übertragung weiterer Sicherheitsanforderungen wie biometrische Systeme, geografische Positionsbestimmung, mit und ohne Zeitabhängigkeiten, sowie separate Zeiteinschränkungen, Netz- und Rechnerdaten u.a. möglicht macht,
   - dass auf dem Server für angemeldete Nutzer ein persönlicher Hauptordner eingerichtet wird, der eine spezielle Datei mit den für diesen Hauptordner festgelegten Sicherheitsanforderungen und Verwaltungsangaben erhält und durch diese spezielle Datei den Status eines Schließfaches erhält,
   - dass in den Hauptordnern weitere Ordner eingerichtet werden können, die nach Funktionen unterschieden werden und durch die spezielle Datei mit den für sie jeweils festgelegten Sicherheitsanforderungen als funktionale Schließfächer fungieren,
   - dass die in den Hauptordnern eingerichteten Schließfächer mindestens die Funktionen persönliche Schließfächer, in die ausschließlich der Nutzer des Hautschließfaches seine Dateien speichern kann und die auch nur diesem Nutzer angezeigt werden, Bereitstellungsschließfächer, in die der Nutzer die Verweise für Dateien in nach Namen unterschiedenen Nutzerschließfächern für andere Anwender ablegt, Empfangsschließfächer, in denen dem Nutzer die mit Namen gekennzeichneten Schließfächer der Absender von Dateien angezeigt werden und beim Öffnen derartiger Schließfächer für den Nutzer ein Verweis zur Ablage der

Dateien und zu den festgelegten Sicherheitsanforderungen sichtbar werden, und öffentliche Schließfächer, in denen vom Nutzer die Verweise auf Dateien gespeichert werden, die bei der Ablage im Bereitstellungsschließfach für mehrere Empfänger vorgesehen sind, und

- dass die Anzeige der Schließfächer nur erfolgt, wenn die sicherheitsrelevanten Vorgaben des Betreibers, Nutzers bzw. Anbieter erfüllt werden, so dass das Schließfachsystem virtuellen Charakter besitzt.

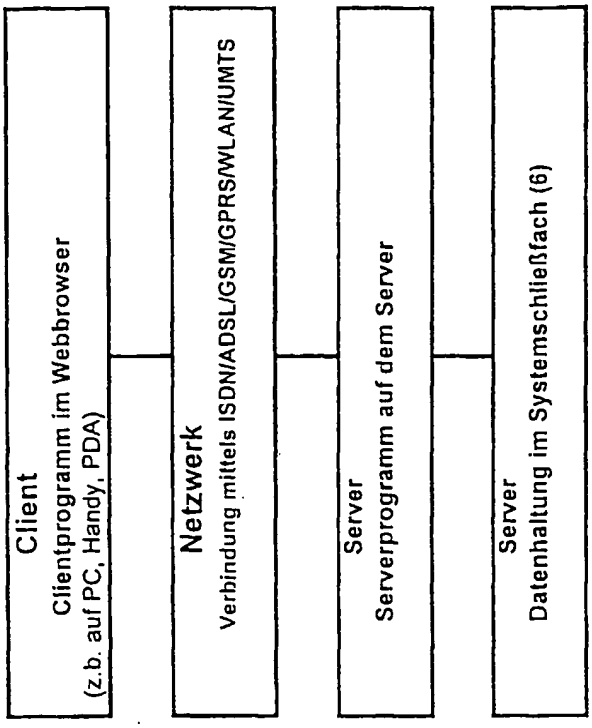

Client
Clientprogramm im Webbrowser
(z.b. auf PC, Handy, PDA)
Netzwerk
Verbindung mittels ISDN/ADSL/GSM/GPRS/WLAN/UMTS
Server
Serverprogramm auf dem Server
Server
Datenhaltung im Systemschließfach (6)

Fig. 1

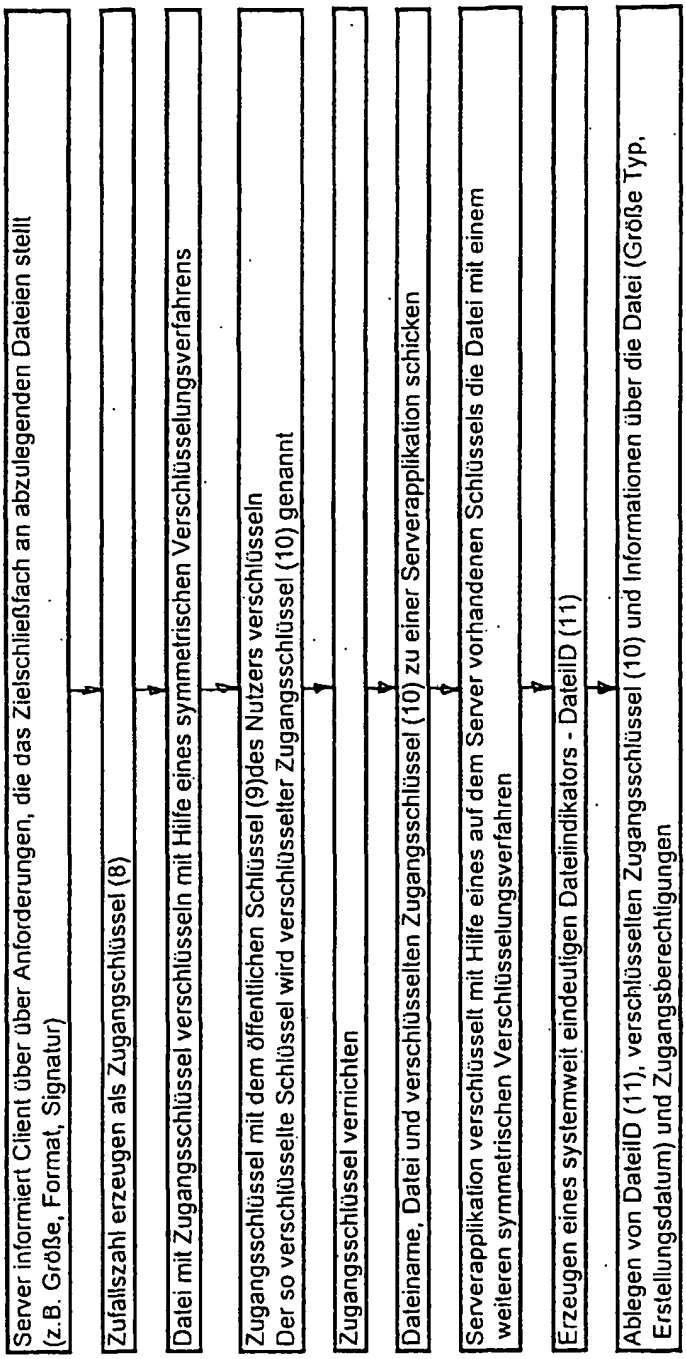

Server informiert Client über über Anforderungen, die das Zielschließfach an abzulegenden Dateien stellt (z.B. Größe, Format, Signatur)
Zufallszahl erzeugen als Zugangschlüssel (8)
Datei mit Zugangsschlüssel verschlüsseln mit Hilfe eines symmetrischen Verschlüsselungsverfahrens
Zugangsschlüssel mit dem öffentlichen Schlüssel (9)des Nutzers verschlüsseln
Der so verschlüsselte Schlüssel wird verschlüsselter Zugangsschlüssel (10) genannt
Zugangsschlüssel vernichten
Dateiname, Datei und verschlüsselten Zugangsschlüssel (10) zu einer Serverapplikation schicken
Serverapplikation verschlüsselt mit Hilfe eines auf dem Server vorhandenen Schlüssels die Datei mit einem weiteren symmetrischen Verschlüsselungsverfahren
Erzeugen eines systemweit eindeutigen Dateiindikators - DateiID (11)
Ablegen von DateiID (11), verschlüsselten Zugangsschlüssel (10) und Informationen über die Datei (Größe Typ, Erstellungsdatum) und Zugangsberechtigungen

Fig. 2

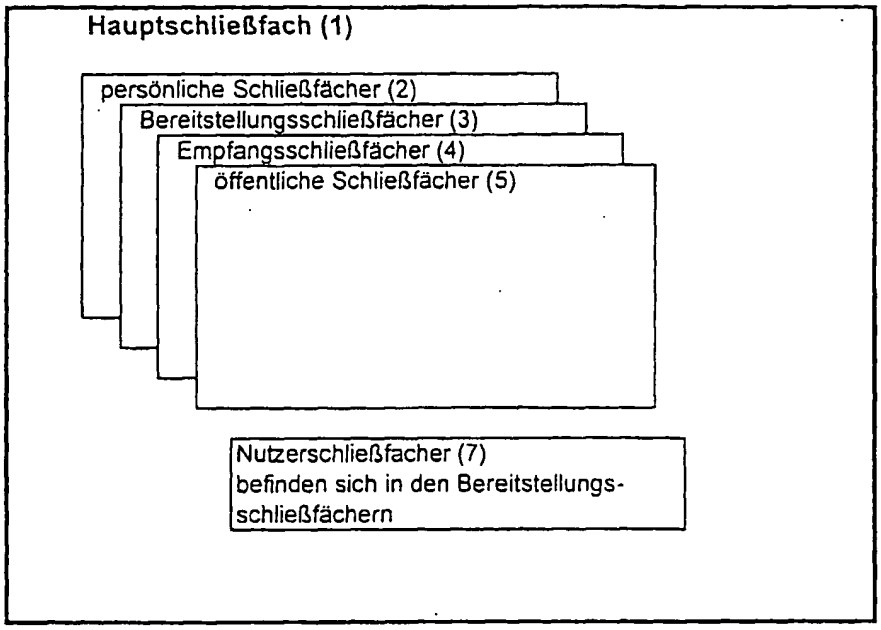

Hauptschließfach (1)
persönliche Schließfächer (2)
Bereitstellungsschließfächer (3)
Empfangsschließfächer (4)
öffentliche Schließfächer (5)
Nutzerschließfacher (7)
befinden sich in den Bereitstellungs-
schließfächern

Fig. 3

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE2004/001252

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 00/51034 A (CLICK2SEND COM INC)<br>31 August 2000 (2000-08-31)<br>the whole document<br>----- | 1 |

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 12 November 2004 | 22/11/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Meis, M |



Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE2004/001252

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 0051034 A | 31-08-2000 | AU 3607100 A | 14-09-2000 |
| | | WO 0051034 A2 | 31-08-2000 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2004/001252

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 7 G06F1/00 G06F17/30

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
IPK 7 G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | WO 00/51034 A (CLICK2SEND COM INC)<br>31. August 2000 (2000-08-31)<br>das ganze Dokument<br>----- | 1 |

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 12. November 2004 | 22/11/2004 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Meis, M |

**INTERNATIONALE RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2004/001252

| Im Recherchenbericht angeführtes Patentdokument | | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | | Datum der Veröffentlichung |
|---|---|---|---|---|---|
| WO 0051034 | A | 31-08-2000 | AU | 3607100 A | 14-09-2000 |
| | | | WO | 0051034 A2 | 31-08-2000 |